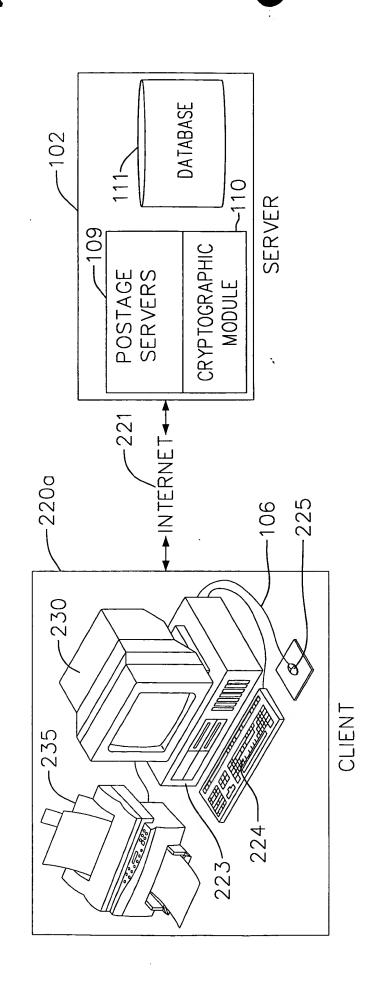
FIG. 1



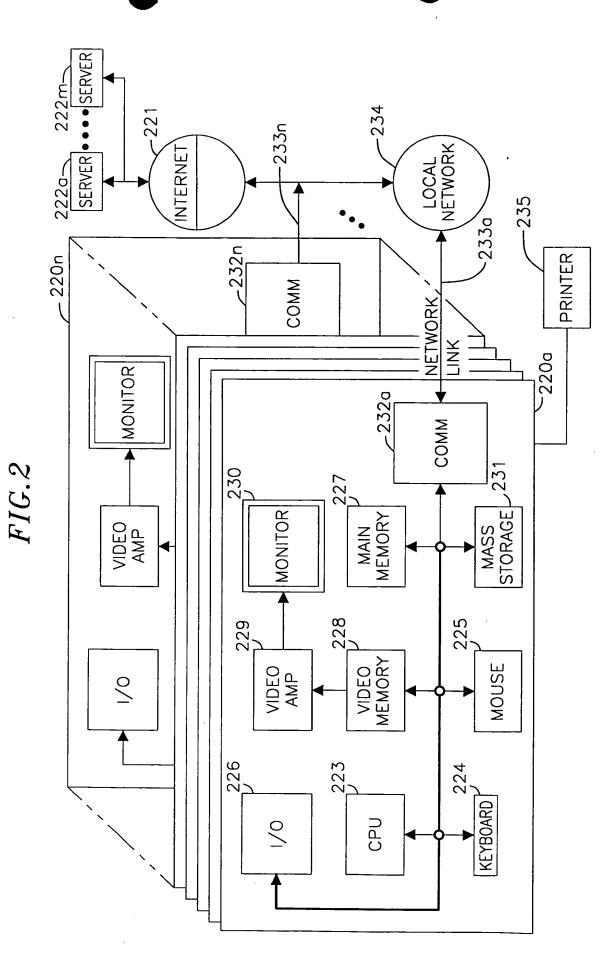
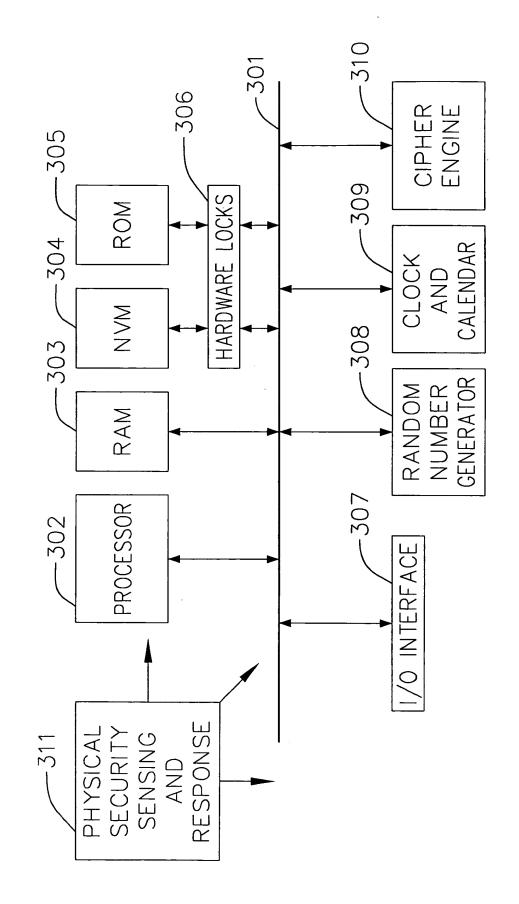
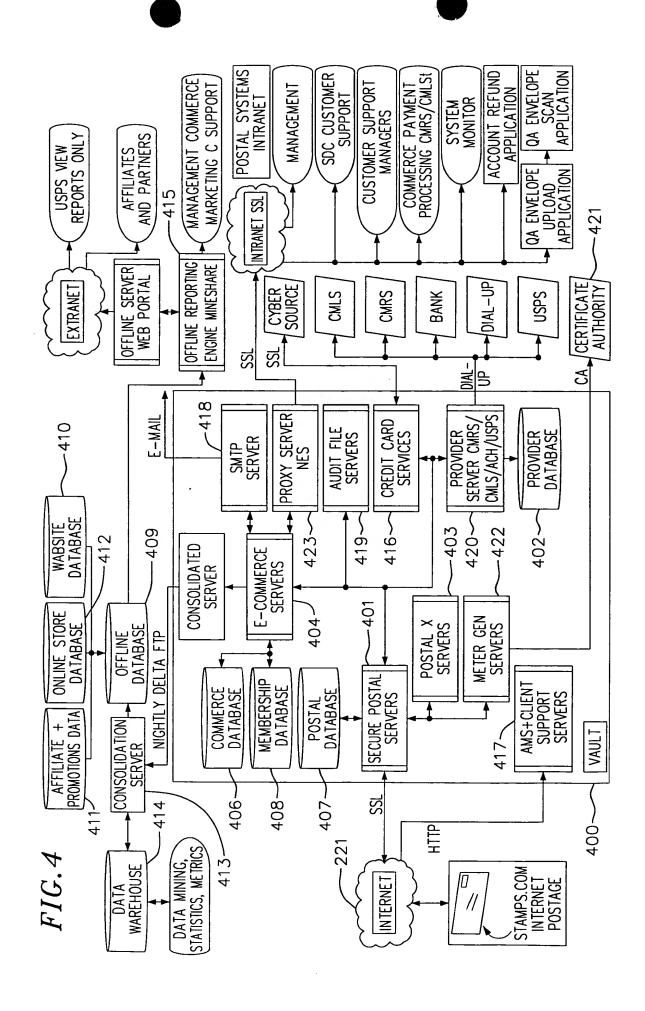


FIG.3





GENERATES A RANDOM, 64-BIT CHALLENGE CLIENT SOFTWARE

THE CHALLENGE IT SENT WITH • COMPARES THE HMAC OF THE HMAC IT RECEIVES FROM THE PSD. CLIENT SOFTWARE

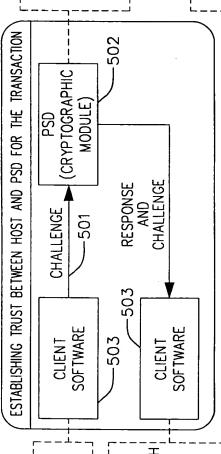
- HOST TRUSTS THE PSD FOR THIS TRANSACTION.
- CHALLENGE TO AUTHENTICATE HOST RETAINS PSD'S ITSELF TO THE PSD

505-

CUSTOMER'S ASCENDING AND SIGNS CHALLENGE THAT THE PSD SENT, AND ALSO THE LOCAL RECORD OF THE DESCENDING REGISTERS. SENDS THIS TO PSD. CLIENT SOFTWARE

SENDS CLEARTEXT OF THE TRANSACTION MESSAGE. CHALLENGE AND THE

SENDS AN HMAC OF ALL OF THE ABOVE, USING SHARED



PSD RETURNS ABOVE, AS WELL AS ITS OWN 64-BIT CHALLENGE

SHARED DURING REGISTRATION

• THE PSD SIGNS THE HOST'S CHALLENGE, USING THE HMK

CALCULATION OF THE SAME WAS NOT TAMPERED WITH. THIS ENSURES MESSAGE RESPONSE WITH LOCAL COMPARES HASH OF

-502

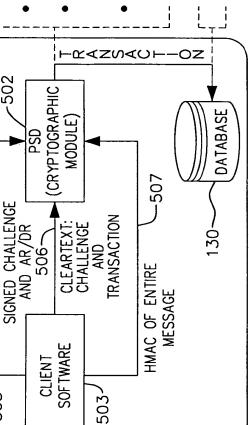
ESTABLISHING TRUST BETWEEN PSD AND HOST FOR -THE TRANSACTION

RECEIVED IS CHALLENGE SENT. VERIFIES HOST'S REGISTERS ARE SAME AS LOCAL DATA **VERIFIES CHALLENGE**

THIS ABOVE TWO STEPS AUTHENTICATE THE

OF REGISTERS.

PSD PERFORMS TRANSACTION



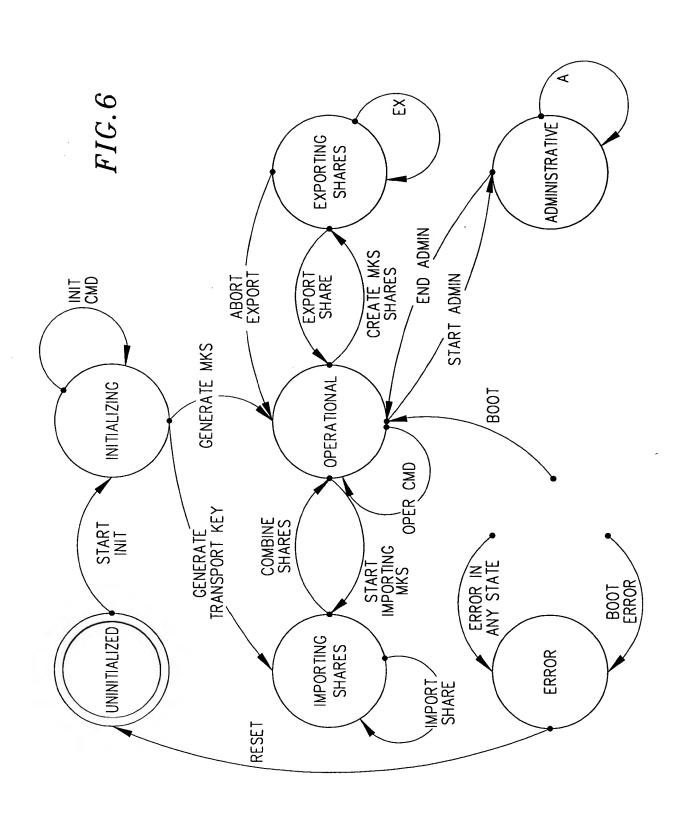
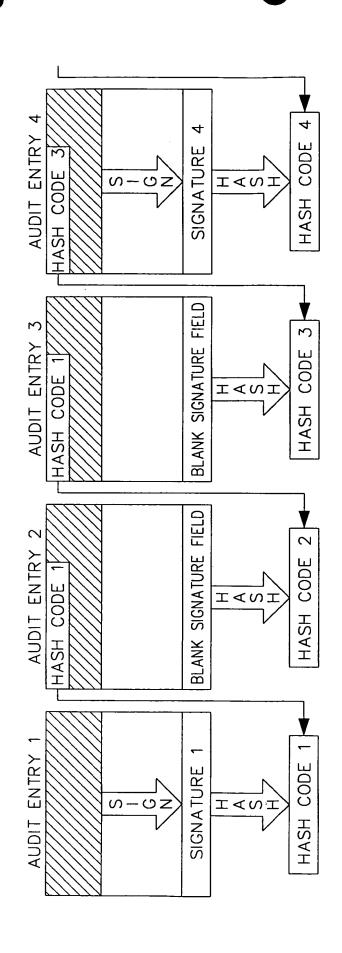
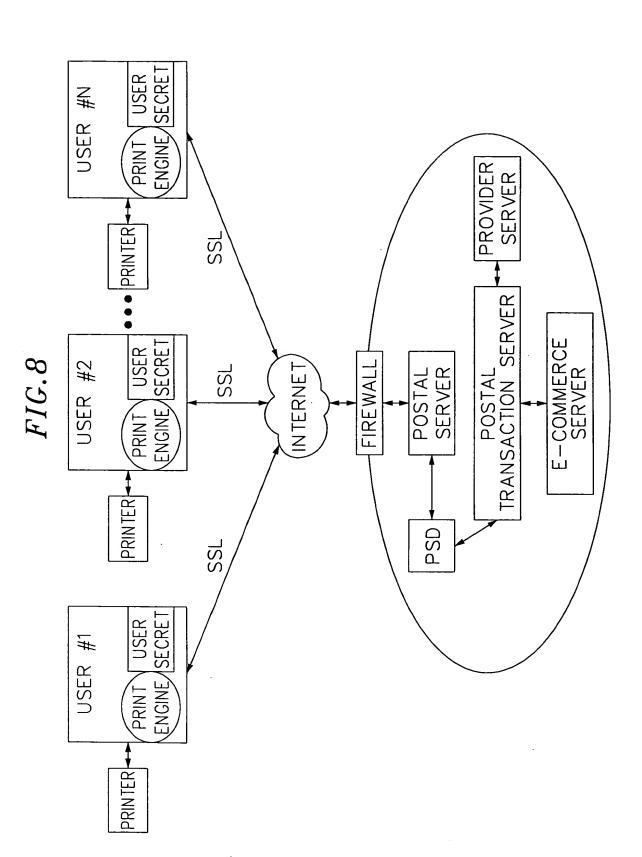


FIG. 7





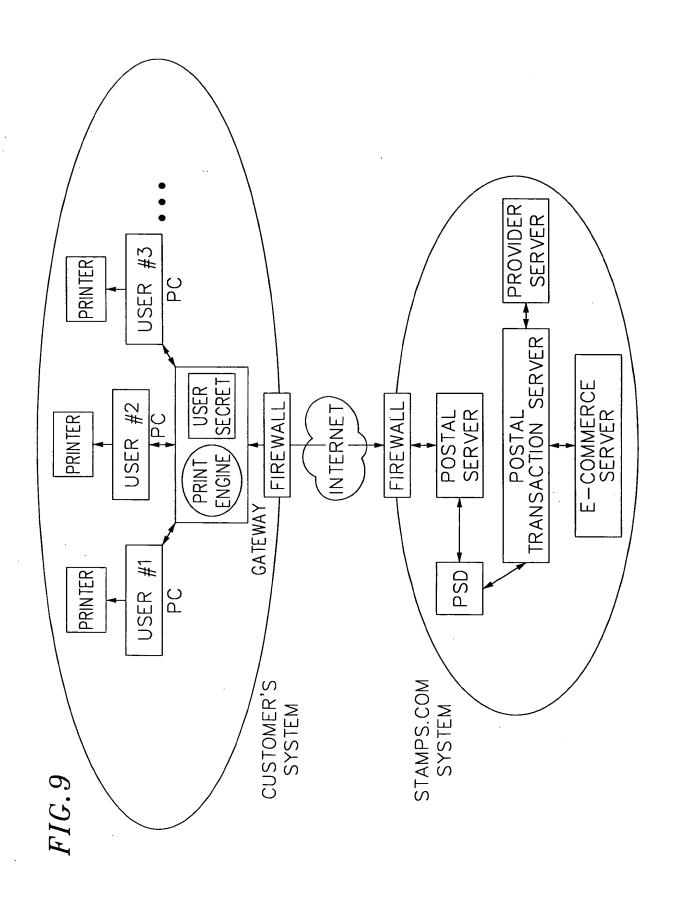


FIG. 10

